U.S. DEPARTMENT OF COMMERCE PATENT & TRADEMARK OFFICE

| B/O Form PTO-1390 **Transmittal Letter to the United States Designated/Elected Office (DO/EO/US) Concerning a Filing Under *35 USC 371*** | | *Attorney's Docket Number* MODL3004/JEK<br>*U.S. Application Number (if known)* 10/030164 |
|---|---|---|
| *International Application Number* PCT/EP00/07124 | *International Filing Date* 25 July 2000 | *Priority Date Claimed* 30 July 1999 |
| *Title of Invention* METHOD, DEVICE AND SYSTEM FOR BIOMETRIC AUTHENTICATION | | |
| *Applicant(s) for DO/EO/US* Albert MÖDL et al. | Assignee | |

**Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items under *35 USC 371*:**

1. ☒ This is a **FIRST** submission of items concerning a filing under *35 USC 371*.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under *35 USC 371*.
3. ☒ This express request to begin national examination procedures *(35 USC 371(f))* at any time rather than delay examination until the expiration of the applicable time limit set in *35 USC 371(b)* and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed *35 USC 371(c)(2)*.
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English *(35 USC 371(c)(2))*.
7. ☒ Amendments to the claims of the International Application under PCT Article 19 *(35 USC 371(c)(3))*
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 *(35 USC 371(c)(3))*.
9. ☒ An oath or declaration of the inventor(s) *(35 USC 371(c)(4))*. ( ☐ Executed ☒ Unexecuted)
10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 *(35 USC 371(c)(5))*.

***Items 11 to 16 below concern other document(s) or information included:***

11. ☐ An Information Disclosure Statement under *37 CFR 1.97* and *1.98*.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with *37 CFR 3.28* and *3.31* is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

JC03 Rec'd PCT/PTO 30 JAN 2002

| Application Number (if Known) | International Application Number | Attorney's Docket Number |
|---|---|---|
| 10/030164 | PCT/EP00/07124 | MODL3003/JEK |

| | Calculations | PTO USE ONLY |
|---|---|---|
| 17. The following fees are submitted:<br>**Basic National Fee *(37 CFR 1.492(a)(1)-(5))*:**<br>☒ Search report has been prepared by the EPO or JPO . . . . . $890.00<br>☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* . . . . . $710.00<br>☐ No International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* but International Search Fee paid to USPTO *(37 CFR 1.445(a)(2))* . . . . . $740.00<br>☐ Neither International Preliminary Examination Fee *(37 CFR 1.482)* nor International Search Fee *(37 CFR 1.445(a)(2))* paid to USPTO . . . . . $1040.00<br>☐ International Preliminary Examination Fee paid to USPTO *(37 CFR 1.482)* and all claims satisfied provisions of PCT Article 33(1)-(4) . . . . . $100.00 | | |
| **ENTER APPROPRIATE BASIC FEE AMOUNT** | $ **890.00** | |
| Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(e))*. | | |

| CLAIMS | NUMBER FILED | NUMBER EXTRA | RATE | | |
|---|---|---|---|---|---|
| Total Claims | 18 -20 = | | × $18.00 | | |
| Independent Claims | 2 -3 = | | × $84.00 | | |
| Multiple Dependent Claims (if applicable) | | | + $280.00 | | |
| **TOTAL OF ABOVE CALCULATIONS** | | | | $ **890.00** | |
| Reduction by ½ for filing by small entity, if applicable. Small Entity Status is asserted pursuant to 37 CFR 1.27 for this application. | | | | | |
| **SUBTOTAL** | | | | $ **890.00** | |
| Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date *(37 CFR 1.492(f))*. | | | | | |
| **TOTAL NATIONAL FEE** | | | | $ **890.00** | |
| Fee for recording the enclosed assignment *(37 CFR 1.21(h))*. The assignment must be accompanied by an appropriate cover sheet *(37 CFR 3.28, 3.31)*. **$40.00** per property. | | | | | |
| **TOTAL FEES ENCLOSED** | | | | $ **890.00** | |
| Amount to be: | | | Refunded: | | |
| | | | Charged: | | |

a. ☒ A check in the amount of **$890.00** to cover the fees is enclosed.

b. ☐ Please charge my **Deposit Account Number 02-0200** in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to **Deposit Account Number 02-0200**. A duplicate copy of this sheet is enclosed.

Note: Where an appropriate time limit under *37 CFR 1.494* or *1.495* has not been met, a petition to revive *(37 CFR 1.137(a) or (b))* must be filed and granted to restore the application to pending status.

**Customer 23364**

**BACON & THOMAS, PLLC**
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 223124-1176
(703) 683-0500

DATE: 30 January 2002

*Respectfully submitted,*

*J. Ernest Kenney*
*Attorney for Applicant*
Registration Number: 19,179

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**International Patent Application No. PCT/EP00/07124**

**PCT/DO/EO/US**

**International Filing Date: 25 July 2000**

**Applicant: Albert MÖDL et al.**

**Attorney Docket: MODL3004/JEK**

**For: METHOD, DEVICE AND SYSTEM FOR BIOMETRIC AUTHENTICATION**

## PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

This paper accompanies documents submitted to establish the U.S. national stage of the above-identified international patent application.

The international patent application was amended under PCT Article 34 and the claims as-amended are annexed to the International Preliminary Examination Report (IPER).

Before calculation of the filing fee and before examination, kindly amend the application documents as follows:

**IN THE CLAIMS**:

Please amend the claims as annexed to the IPER as shown on the appended APPENDIX OF CLAIMS, which includes amended and non-amended claims. Also appended hereto an APPENDIX OF MARKED UP CLAIMS showing the changes which have been made.

**IN THE SPECIFICATION:**

In the original specification as-filed, on page 2, change the first partial paragraph on this page to read:

International Application No. PCT/EP00/07124
Attorney Docket: MODL3004/JEK

--data with a person's newly detected biometric data yields a match higher than said (second) threshold value. If the error message is issued it may also be provided that further operation is automatically disabled.--

A marked up version of the amended page 2 of the specification is appended hereto.

In the ANNEX pages submitted as AMENDED SHEETS 1 and 1a, correct the number appearing at the top of the second page to read --1a--.

A marked up version of the second page of the amended sheet of specification is appended hereto.

## REMARKS

All rights are reserved to the original claimed subject matter. The claims have been amended to reduce the filing fees and to restate the inventive subject matter in clear terms. None of the amendments are intended to narrow any element of the claims as they stood prior to amendment. Examination of the application as amended is respectfully requested.

Respectfully submitted,
BACON & THOMAS, PLLC

J. ERNEST KENNEY
Attorney for Applicant
Registration No. 19,179

Customer 23364

**BACON & THOMAS, PLLC**
**625 Slaters Lane - 4th Floor**
**Alexandria, VA 22314-1176**
**Telephone: (703) 683-0500**
**Facsimile: (703) 683-1080**

Date: January 30, 2002
S:\Producer\jek\MODL - MODL3004\preliminary amendment.wpd



International Application No. PCT/EP00/01724
Attorney Docket: MODL3004/JEK



## APPENDIX OF CLAIMS

1. A method for protecting biometric authentication from replay attacks wherein comparison is performed for a match between a person's biometric data stored as reference data and the person's redetected biometric data and authentication is effected if the match is equal to or greater than a predetermined first threshold value, characterized in that authentication is refused if the comparison yields a match of the redetected biometric data with the stored reference data which is equal to or greater than a predetermined second threshold value.

2. A method according to claim 1, characterized in that the second threshold value is defined as a 100% match.

3(Amended). A method according to claim 1, characterized in that the biometric data detected in different authentication processes are collected and stored as data records and authentication is refused if the redetected biometric data of a current authentication process have a match higher than the predetermined second threshold value in comparison to one of the stored data records.

4(Amended). A method according to claim 1, characterized in that the second threshold value is defined as an at least 99% data match.

5(Amended). A method according to claim 1, characterized in that the reference data and optionally the data records are stored on a data carrier, in particular a smart card.

6(Amended). A method according to claim 1, characterized in that the reference data and optionally the data records are stored in an authentication apparatus, in particular a smart card terminal.

7(Amended). A method according to claim 1, characterized in that a hash value is formed from the redetected biometric data, and the stored reference data are a hash value.

8. An apparatus for biometric authentication comprising a first memory area with biometric data as reference data and a comparison circuit which generates a message permitting authentication when a comparison of the reference data with a person's newly detected biometric data yields a match which is equal to or greater than a given first threshold value, characterized in that the comparison circuit generates a message refusing authentication if a comparison of the reference data with a person's newly detected biometric data yields a match which is equal to or greater than a given second threshold value.

9. An apparatus according to claim 8, characterized in that the apparatus is a data carrier, in particular a smart card.

10(Amended). An apparatus according to claim 8, characterized in that the threshold value is set at 100%.

11(Amended). An apparatus according to claim 8, characterized by further memory areas in which several data records of redetected biometric data are stored.

12. An apparatus according to claim 11, characterized in that the further memory areas form a stack.

13. An apparatus according to claim 11, characterized in that the further memory areas form a shift register.

14(Amended). An apparatus according to claim 8, characterized in that the

threshold value is set at a value = 99%.

15(Amended). An apparatus according to claim 8, characterized in that the apparatus is automatically disabled if the message is present.

16(Amended). An apparatus according to claim 8, characterized in that the apparatus issues an error message if the message is present.

17(Amended). An apparatus according to claim 8, characterized in that a hash value derived from biometric data is stored as reference data in the first memory area, and the comparison circuit forms a hash value from the newly detected biometric data for comparison with the stored reference data.

18(Amended). An apparatus according to claim 8, characterized in that the apparatus has a device for detecting a person's biometric data.

S:\Producer\jek\MODL - MODL3004\appendix of claims.wpd



International Application No. PCT/EP00/01724
Attorney Docket: MODL3004/JEK



## APPENDIX OF MARKED UP VERSION OF CLAIMS

3(Amended). A method according to [either of claims 1 and 2] claim 1, characterized in that the biometric data detected in different authentication processes are collected and stored as data records and authentication is refused if the redetected biometric data of a current authentication process have a match higher than the predetermined second threshold value in comparison to one of the stored data records.

4(Amended). A method according to [any of claims 1 to 3] claim 1, characterized in that the second threshold value is defined as an at least 99% data match.

5(Amended). A method according to [any of claims 1 to 4] claim 1, characterized in that the reference data and optionally the data records are stored on a data carrier, in particular a smart card.

6(Amended). A method according to [any of claims 1 to 4] claim 1, characterized in that the reference data and optionally the data records are stored in an authentication apparatus, in particular a smart card terminal.

7(Amended). A method according to [any of claims 1 to 6] claim 1, characterized in that a hash value is formed from the redetected biometric data, and the stored reference data are a hash value.

10(Amended). An apparatus according to claim 8 [or 9], characterized in that the threshold value is set at 100%.

11(Amended). An apparatus according to [any of claims 8 to 10] claim 8, characterized by further memory areas in which several data records of redetected biometric data are stored.

14(Amended). An apparatus according to [any of claims 8 to 13] claim 8, characterized in that the threshold value is set at a value = 99%.

15(Amended). An apparatus according to [any of claims 8 to 14] claim 8, characterized in that the apparatus is automatically disabled if the message is present.

16(Amended). An apparatus according to [any of claims 8 to 15] claim 8, characterized in that the apparatus issues an error message if the message is present.

17(Amended). An apparatus according to [any of claims 8 to 16] claim 8, characterized in that a hash value derived from biometric data is stored as reference data in the first memory area, and the comparison circuit forms a hash value from the newly detected biometric data for comparison with the stored reference data.

18(Amended). An apparatus according to [any of claims 8 to 17] claim 8, characterized in that the apparatus has a device for detecting a person's biometric data.

message and for example issues an error message when a comparison of the reference data with a person's newly detected biometric data yields a match higher than said (second) threshold value. If the error message is issued it may also be provided that further operation is automatically disabled.

An example to be mentioned is the comparison of two signatures by one and the same person. Said signatures may be congruent when viewed visually, but they can never be brought in congruence pixel by pixel at a resolution of 500 dpi for example. If the dynamic components of the signature are taken into consideration there are further degrees of freedom and natural deviations.

This (second) threshold value of 99% or 100% relevant for the invention is stored together with the reference data either in a terminal or on a separate data carrier, in particular a smart card.

In a preferred embodiment of the invention it is provided that the detected biometric data which led to an authentication, and optionally also those detected biometric data which did not lead to authentication because they were below the first threshold value, are collected and stored as data records. Said data records are preferably stored in a stack or shift register. In each authentication process it is then checked whether the biometric data of the presented biometric feature are identical with one of the stored data records or optionally have more than a 99% match. Then a replay attack can be assumed and authentication is refused by the authentication system.

In a further advantageous embodiment of the invention, hash values are stored instead of, or in addition to, the biometric comparative data records last received by the smart card. A hash function is applied to the comparative data record to generate a relatively short hash value. Hash functions are known in the art, a hash function being a unique, reductive mapping onto a fixed-length word. The hash function is executed in several rounds on a block-by-block partition of the raw data. The result depends on the total input. Calculation of the raw data from the hash value is not possible. It is difficult in terms of complexity theory to alter the input data selectively in such a way that the hash value remains the same.

such a great match a replay attack can be assumed, and authentication is therefore refused according to the invention. A comparison circuit is provided which generates a message and for example issues an error message when a comparison of the reference

# TRANSLATION OF

# ANNEXES

# TO IPER

# FOR

# PCT/EP00/07124

Method and apparatus for biometric authentication

This invention relates to a method and to an apparatus for biometric authentication, in particular for protecting biometric authentication from replay attacks.

An authentication method is used when a person desires access to protected facilities. For example, authentication is regularly effected by means of a PIN comparison when a card user introduces a smart card - for example a credit card - into a bank machine (terminal) or when a person desires admission to protected-access premises. A stored PIN is checked for identity with the PIN entered by the card user or the person desiring admission.

In the case of a biometric authentication method, a biometric feature of the person is used as an identification feature instead of a PIN. The biometric feature can be a fingerprint, for example, but shall also include a personal signature within the scope of the present invention. A disadvantage of such authentication methods is that an attack on authentication is possible if the biometric data which were stored as reference data or which led to an authentication are intercepted by unauthorized third parties to be used again later for unauthorized authentication. This type of attack is referred to as a replay attack. WO 98/11750 A2 discloses a method for preventing replay attacks wherein the encrypted digital data of fingerprints are stored. If identical data are entered at a later time, authentication is refused.

The problem of the present invention is therefore to provide a method and apparatus for biometric authentication methods with better protection from replay attacks.

This problem is solved according to the invention by the features of the independent claims. Subclaims state advantageous embodiments of the invention.

The invention exploits the fact that biometric features normally have in common that they are not 100% reproducible, unlike the PIN, so that authorization is already effected if the match of the biometric feature presented by the person with the stored reference data exceeds a predetermined threshold value. It is now provided according to the invention that the match must not be above a (second) predetermined threshold value, in particular must not be 100% and preferably no more than 99%. In the case of

such a great match a replay attack can be assumed, and authentication is therefore refused according to the invention. A comparison circuit is provided which generates a message and for example issues an error message when a comparison of the reference

Claims

1. A method for protecting biometric authentication from replay attacks wherein comparison is performed for a match between a person's biometric data stored as reference data and the person's redetected biometric data and authentication is effected if the match is equal to or greater than a predetermined first threshold value, characterized in that authentication is refused if the comparison yields a match of the redetected biometric data with the stored reference data which is equal to or greater than a predetermined second threshold value.

2. A method according to claim 1, characterized in that the second threshold value is defined as a 100% match.

3. A method according to either of claims 1 and 2, characterized in that the biometric data detected in different authentication processes are collected and stored as data records and authentication is refused if the redetected biometric data of a current authentication process have a match higher than the predetermined second threshold value in comparison to one of the stored data records.

4. A method according to any of claims 1 to 3, characterized in that the second threshold value is defined as an at least 99% data match.

5. A method according to any of claims 1 to 4, characterized in that the reference data and optionally the data records are stored on a data carrier, in particular a smart card.

6. A method according to any of claims 1 to 4, characterized in that the reference data and optionally the data records are stored in an authentication apparatus, in particular a smart card terminal.

7. A method according to any of claims 1 to 6, characterized in that a hash value is formed from the redetected biometric data, and the stored reference data are a hash value.

8. An apparatus for biometric authentication comprising a first memory area with biometric data as reference data and a comparison circuit which generates a message permitting authentication when a comparison of the reference data with a person's newly detected biometric data yields a match which is equal to or greater than a given

first threshold value, characterized in that the comparison circuit generates a message refusing authentication if a comparison of the reference data with a person's newly detected biometric data yields a match which is equal to or greater than a given second threshold value.

9. An apparatus according to claim 8, characterized in that the apparatus is a data carrier, in particular a smart card.

10. An apparatus according to claim 8 or 9, characterized in that the threshold value is set at 100%.

11. An apparatus according to any of claims 8 to 10, characterized by further memory areas in which several data records of redetected biometric data are stored.

12. An apparatus according to claim 11, characterized in that the further memory areas form a stack.

13. An apparatus according to claim 11, characterized in that the further memory areas form a shift register.

14. An apparatus according to any of claims 8 to 13, characterized in that the threshold value is set at a value = 99%.

15. An apparatus according to any of claims 8 to 14, characterized in that the apparatus is automatically disabled if the message is present.

16. An apparatus according to any of claims 8 to 15, characterized in that the apparatus issues an error message if the message is present.

17. An apparatus according to any of claims 8 to 16, characterized in that a hash value derived from biometric data is stored as reference data in the first memory area, and the comparison circuit forms a hash value from the newly detected biometric data for comparison with the stored reference data.

18. An apparatus according to any of claims 8 to 17, characterized in that the apparatus has a device for detecting a person's biometric data.

# Method, apparatus and system for biometric authentication

This invention relates to a method and to an apparatus and system for biometric authentication, in particular for protecting biometric authentication from replay attacks.

An authentication method is used when a person desires access to protected facilities. For example, authentication is regularly effected by means of a PIN comparison when a card user introduces a smart card - for example a credit card - into a bank machine (terminal) or when a person desires admission to protected-access premises. A stored PIN is checked for identity with the PIN entered by the card user or the person desiring admission.

In the case of a biometric authentication method, a biometric feature of the person is used as an identification feature instead of a PIN. The biometric feature can be a fingerprint, for example, but shall also include a personal signature within the scope of the present invention. A disadvantage of such authentication methods is that an attack on authentication is possible if the biometric data which were stored as reference data or which led to an authentication are intercepted by unauthorized third parties to be used again later for unauthorized authentication. This type of attack is referred to as a replay attack.

The problem of the present invention is therefore to protect biometric authentication methods from replay attacks.

This problem is solved according to the invention by the features of the independent claims. Subclaims state advantageous embodiments of the invention.

The invention exploits the fact that biometric features normally have in common that they are not 100% reproducible, unlike the PIN, so that authorization is already effected if the match of the biometric feature presented by the person with the stored reference data exceeds a predetermined threshold value. It is now provided according to the invention that the match must not be above a (second) predetermined threshold value, in particular must not be 100% and preferably no more than 99%. In the case of such a great match a replay attack can be assumed, and authentication is therefore refused according to the invention. A comparison circuit is provided which generates a

message and for example issues an error message when a comparison of the reference data with a person's newly detected biometric data yields a match higher than said (second) threshold value. If the error message is issued it may also be provided that further operation is automatically disabled.

An example to be mentioned is the comparison of two signatures by one and the same person. Said signatures may be congruent when viewed visually, but they can never be brought in congruence pixel by pixel at a resolution of 500 dpi for example. If the dynamic components of the signature are taken into consideration there are further degrees of freedom and natural deviations.

This (second) threshold value of 99% or 100% relevant for the invention is stored together with the reference data either in a terminal or on a separate data carrier, in particular a smart card.

In a preferred embodiment of the invention it is provided that the detected biometric data which led to an authentication, and optionally also those detected biometric data which did not lead to authentication because they were below the first threshold value, are collected and stored as data records. Said data records are preferably stored in a stack or shift register. In each authentication process it is then checked whether the biometric data of the presented biometric feature are identical with one of the stored data records or optionally have more than a 99% match. Then a replay attack can be assumed and authentication is refused by the authentication system.

In a further advantageous embodiment of the invention, hash values are stored instead of, or in addition to, the biometric comparative data records last received by the smart card. A hash function is applied to the comparative data record to generate a relatively short hash value. Hash functions are known in the art, a hash function being a unique, reductive mapping onto a fixed-length word. The hash function is executed in several rounds on a block-by-block partition of the raw data. The result depends on the total input. Calculation of the raw data from the hash value is not possible. It is difficult in terms of complexity theory to alter the input data selectively in such a way that the hash value remains the same.

If features are presented a further time and biometric data calculated therefrom are brought into the card, the hash value is recalculated. The likelihood of two biometric data records generating the same hash value is low, so that a replay attack must be assumed in case of a match. The use of hash values permits considerable savings of memory space and processing time in realization of the invention. It is easy to store several fixed-length hash values in a kind of shift register here since a hash value usually requires only a few bytes of memory space.

Claims

1. A method for protecting biometric authentication from replay attacks wherein comparison is performed for a match between a person's biometric data stored as reference data and the person's redetected biometric data and authentication is effected on the basis of said comparison, characterized in that authentication is refused if the comparison yields a match of the redetected biometric data with the stored reference data which is equal to or greater than a predetermined threshold value.

2. A method according to claim 1, characterized in that the threshold value is defined as a 100% match.

3. A method according to either of claims 1 and 2, characterized in that the biometric data detected in different authentication processes are collected and stored as data records and authentication is refused if the redetected biometric data of a current authentication process have a match higher than the predetermined threshold value in comparison to one of the stored data records.

4. A method according to any of claims 1 to 3, characterized in that the threshold value is defined as an at least 99% data match.

5. A method according to any of claims 1 to 4, characterized in that the reference data and optionally the data records are stored on a data carrier, in particular a smart card.

6. A method according to any of claims 1 to 4, characterized in that the reference data and optionally the data records are stored in an authentication apparatus, in particular a smart card terminal.

7. A method according to any of claims 1 to 6, characterized in that a hash value is formed from the redetected biometric data, and the stored reference data are a hash value.

8. An apparatus for biometric authentication comprising a first memory area with biometric data as reference data and a comparison circuit which generates a message when a comparison of the reference data with a person's newly detected biometric data yields a match which is equal to or greater than a given threshold value.

9. An apparatus according to claim 8, characterized in that the apparatus is a data carrier, in particular a smart card.

10. An apparatus according to claim 8 or 9, characterized in that the threshold value is set at 100%.

11. An apparatus according to any of claims 8 to 10, characterized by further memory areas in which several data records of redetected biometric data are stored.

12. An apparatus according to claim 11, characterized in that the further memory areas form a stack.

13. An apparatus according to claim 11, characterized in that the further memory areas form a shift register.

14. An apparatus according to any of claims 8 to 13, characterized in that the threshold value is set at a value = 99%.

15. An apparatus according to any of claims 8 to 14, characterized in that the apparatus is automatically disabled if the message is present.

16. An apparatus according to any of claims 8 to 15, characterized in that the apparatus issues an error message if the message is present.

17. An apparatus according to any of claims 8 to 16, characterized in that a hash value derived from biometric data is stored as reference data in the first memory area, and the comparison circuit forms a hash value from the newly detected biometric data for comparison with the stored reference data.

18. A system for biometric authentication comprising an apparatus according to any of claims 8 to 17 and a device for detecting a person's biometric data.

## Abstract

A method, apparatus and system for biometric authentication are proposed which are protected from replay attacks. In biometric authentication, a biometric feature presented by a person, for example a fingerprint or the personal signature, is presented and compared with previously stored reference data. In order to prevent the biometric data from being intercepted and used again for unauthorized authentication, the invention provides that authentication is refused in case of a 100% match or only 99% match of the data of the presented biometric feature with the stored reference data. This is because biometric features normally have the property that they cannot be detected in 100% reproducible fashion so that in such cases a replay attack can be assumed. In one embodiment of the invention, the presented biometric features are collected and stored and taken into account in subsequent authentication methods in the check for replay attacks.

10030164 - 042502

#3

ATTORNEY/DOCKET NO: **MODL3004/JEK**

# DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention (Design, if applicable) entitled:

**METHOD, DEVICE AND SYSTEM FOR BIOMETRIC AUTHENTICATION**

the specification of which (check one):

☐ is attached hereto, or ☒ was filed on: **25 July 2000** as U.S. Application Number or PCT International Application Number: **(PCT/EP00/07124) 10/030,164** and (if applicable) was amended on:

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56.* I hereby claim foreign priority benefits under *Title 35, United States Code §119* of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

| PRIOR FOREIGN APPLICATION(S) | | | PRIORITY CLAIMED | |
|---|---|---|---|---|
| Number | Country | Day/Month/Year Filed | Yes | No |
| 199 36 094.4 | Germany | 30 July 1999 | X | |
| | | | | |

☐ Additional Priority Application(s) Listed on Following Page(s)

| I HEREBY CLAIM THE BENEFIT UNDER TITLE 35 U.S. CODE §119(E) OF ANY U.S. PROVISIONAL APPLICATIONS LISTED BELOW. | |
|---|---|
| Application Number | Day/Month/Year Filed |
| | |
| | |

☐ Additional Provisional Application(s) Listed on Following Page(s)

I hereby claim the benefit under *Title 35, United States Code, §120* of any United States application(s) or PCT international application(s) designating The United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of *Title 35, United States Code, §112*, I acknowledge the duty to disclose information which is material to patentability as defined in *Title 37, Code of Federal Regulations, §1.56* which became available between the filing date of the prior application(s) and the national or PCT international filing date of this application:

| Application Number | Filing Date | Status - Patented, Pending or Abandoned |
|---|---|---|
| | | |
| | | |

☐ Additional US/PCT Priority Application(s) listed on Following Page(s)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under *section 1001 of title 18 of the United States Code* and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(6) POWER OF ATTORNEY: I (We) hereby appoint as my (our) attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: J. Ernest Kenney, Reg. No. 19,179; Eugene Mar, Reg. No. 25,893; Richard E. Fichter, Reg. No. 26,382; Thomas J. Moore, Reg. No. 28,974; Joseph DeBenedictis, Reg. No. 28,502; Benjamin E. Urcia, Reg. No. 33,805; and

I(we) authorize my(our) attorneys to accept and follow instructions from **Klunker, Schmitt-Nilson, Hirsch** regarding any matter related to the preparation, examination, grant and maintenance of this application, any continuation, continuation-in-part or divisional based thereon, and any patent resulting therefrom, until I(we) or my(our) assigns withdraw this authorization in writing.

Send correspondence to: **Customer 23364**

**BACON & THOMAS, PLLC**
**625 Slaters Lane - 4th Floor**
**Alexandria, VA 22314-1176**

Telephone Calls to: **J. Ernest Kenney**
**(703) 683-0500**

1-00

| FULL NAME OF FIRST OR SOLE INVENTOR | CITIZENSHIP |
|---|---|
| **Albert MÖDL** | Germany |
| RESIDENCE ADDRESS<br>Walter-Kollo-Strasse 21, D-86368 Gersthofen, Germany<br>DEX | POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW |
| DATE<br>X 22 March 2002 | SIGNATURE<br>X Albert Mödl |

☒ *See following page(s) for additional joint inventors.*

ATTORNEY/DOCKET NO: **MODL3004/JEK**

# CONTINUATION OF DECLARATION FOR PATENT APPLICATION AND APPOINTMENT OF ATTORNEY



| PRIOR FOREIGN APPLICATION(S) (35 USC §119) | | | PRIORITY CLAIMED | |
|---|---|---|---|---|
| **Number** | **Country** | **Day/Month/Year Filed** | **Yes** | **No** |
| | | | | |
| | | | | |

| PRIOR PROVISIONAL APPLICATIONS 35 U.S. CODE §119(E) | |
|---|---|
| **Application Number** | **Day/Month/Year Filed** |
| | |
| | |

| PRIOR U.S. OR PCT INTERNATIONAL APPLICATIONS (35 U.S. CODE §120) | | |
|---|---|---|
| **Application Number** | **Filing Date** | **Status - Patented, Pending or Abandoned** |
| | | |
| | | |

2-00

| FULL NAME OF JOINT INVENTOR | CITIZENSHIP |
|---|---|
| **Elmar STEPHAN** | Germany |
| RESIDENCE ADDRESS<br>Danklstrasse 13, D-81~~371 Munchen~~, Germany DEX | POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW |
| DATE<br>X 22 March 2002 | SIGNATURE<br>X |

3-00

| FULL NAME OF JOINT INVENTOR | CITIZENSHIP |
|---|---|
| **Robert MÜLLER** | Germany |
| RESIDENCE ADDRESS<br>Hansjakobstrasse 80, D-~~81673 Munchen~~, Germany DEX | POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW |
| DATE<br>X 22 March 2002 | SIGNATURE<br>X |

| FULL NAME OF JOINT INVENTOR | CITIZENSHIP |
|---|---|
| RESIDENCE ADDRESS | POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW |
| DATE | SIGNATURE |

| FULL NAME OF JOINT INVENTOR | CITIZENSHIP |
|---|---|
| RESIDENCE ADDRESS | POST OFFICE ADDRESS IS THE SAME AS RESIDENCE ADDRESS UNLESS OTHERWISE SHOWN BELOW |
| DATE | SIGNATURE |

☐ *See following pages for additional joint inventors/priority applications.*